

The DSHS logo is in a bold, yellow, sans-serif font. It is positioned on the left side of a horizontal banner that features a blurred background image of a diverse group of people. The banner has a yellow stripe at the bottom.

**DSHS**

The ProviderOne logo consists of the word "Provider" in a bold, black, sans-serif font, followed by a stylized graphic of two overlapping triangles (one blue, one green) and the word "one" in a black, sans-serif font. Below the logo, the text "Washington's Social and Health Services Provider Payment System" is written in a smaller, black, sans-serif font.

**ProviderOne**  
Washington's Social and Health Services Provider Payment System

# **MCO/RSN Testing**

## *Updated*

Presented May 4, 2009  
*Updated June 16, 2009*

# Topics to be covered

- **Testing**
  - Scope of testing, critical dates, key testing terms
  
- **Pre-requisites for testing**
  - How to prepare for testing
  
- **Accessing ProviderOne after Go Live**
  - Security set-up and User Training

# Scope of Testing

## ■ 837 Encounter File - *Format* Compliance

- Called “EDI 1” testing - Tests the 837 encounter file for format compliance – levels 1, 2 and 7 in Edifecs EDI gateway tool
- Timing: Available

## ■ 837 Encounter File – *Content* Compliance

- Called “EDI 2” testing - Tests the 837 encounter file for content compliance – MCO or RSN specific edits on encounter file
- Timing: 6/15 – 8/26

## ■ 834 Enrollment Roster and 820 Premium Payment

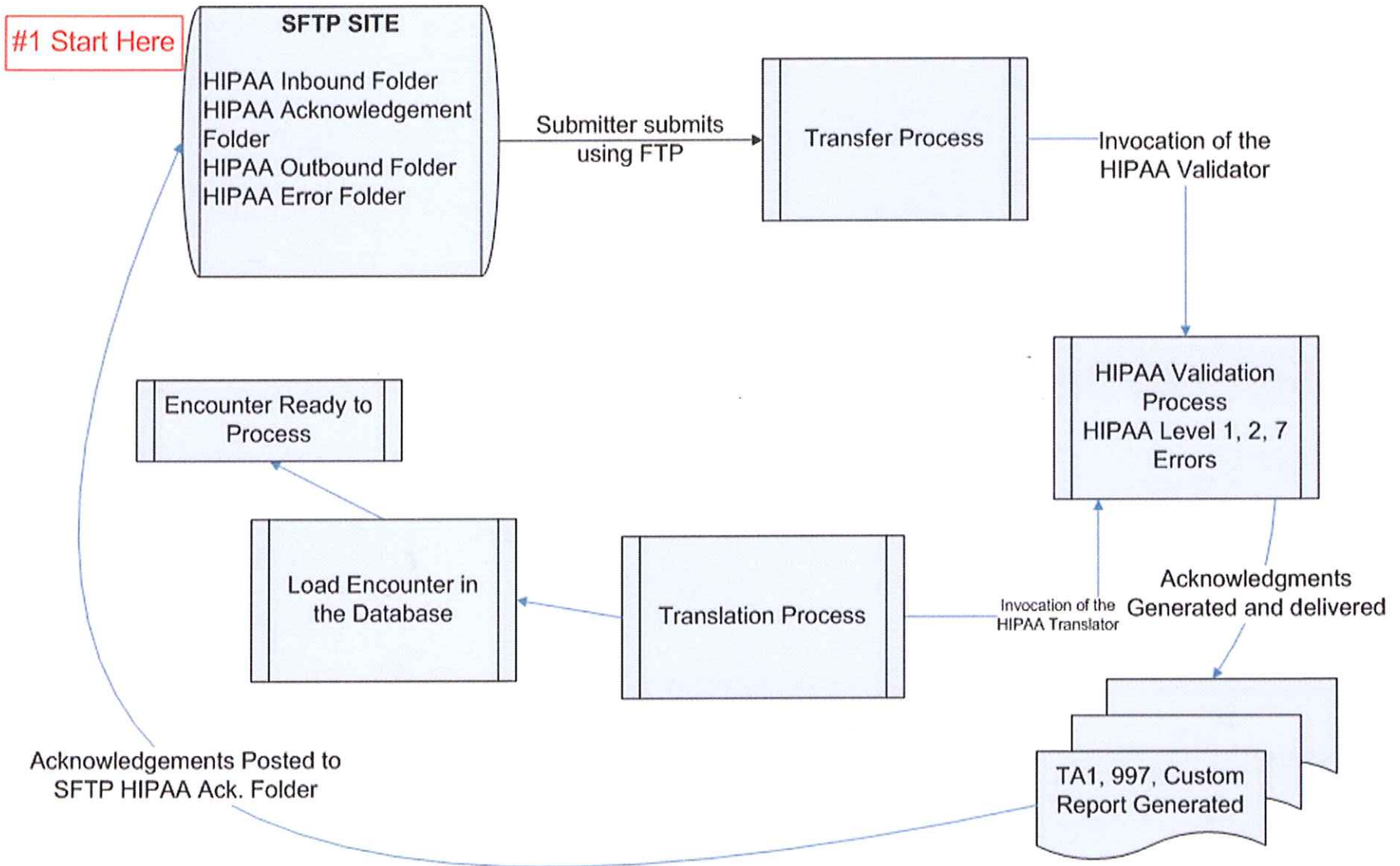
- Retrieve files from Secure File Transfer Protocol (SFTP) site and process within your internal systems
- Timing: early July – 8/26 (schedule distributed at conference call 7/8/09 MCOs and 7/9/09 RSNS)



# Scope of Testing, cont.

Testing	Description	Timing
837 encounter – format compliance	Verifies compliance with Levels 1, 2 and 7 of Edifecs gateway tool	Available now
837 encounter – content compliance	Verifies compliance with MCO or RSN specific edits	6/15-8/28
834 enrollment roster/ 820 premium payment	Retrieve and process 834 and 820 files from SFTP site	Early July

# SFTP Overview



# Important Testing Terms



## ■ TA1 Envelope Acknowledgment

- All submitted files receive a TA1. If an error occurs in the envelope, the file is not processed further. The submitter must correct the error and resubmit the file for further processing.

## ■ 997 Functional Acknowledgement

- All submitted files having a positive TA1 receive either a positive or negative 997.
- Positive 997: A positive 997 and Custom Report are generated for each file that passes the header and trailer check and the HIPAA Level 1, 2 and 7 editing.
- Negative 997: A negative 997 and Custom Report is generated when HIPAA Level 1, 2 and 7 errors occur in the file.

## ■ Custom Report

- All submitted files having a positive TA1 and 997 receive a Custom Report.



# How to Interpret 837 Responses

Submitter Initial Action	System Action	Submitter Requirement	Submitter Action - 2
Encounter file submitted	Submitter receives: <ul style="list-style-type: none"> <li>▪ Negative TA1</li> <li>▪ No 997</li> <li>▪ No Custom Report</li> </ul> Identifies HIPAA level 1, 2, or 7 errors in the envelope (Header and/or Trailer)	Submitter verifies and corrects envelope level errors	File is resubmitted
Encounter file submitted	Submitter receives: <ul style="list-style-type: none"> <li>▪ Positive TA1</li> <li>▪ Negative 997</li> <li>▪ Negative Custom Report</li> </ul> Identifies HIPAA level 1, 2, or 7 errors in the file detail	Submitter verifies and corrects detail level errors	File is resubmitted
Encounter file submitted	Submitter receives: <ul style="list-style-type: none"> <li>▪ Positive TA1</li> <li>▪ Positive 997</li> <li>▪ Positive Custom Report</li> </ul> Identifies <u>no</u> HIPAA level 1, 2, or 7 errors at envelope or detail levels	File moves forward for encounter record processing (edits)	ETRR generated

# **Pre-Requisites for Testing - Summary**

- 1. Modify systems to Companion Guides**
- 2. ProviderOne client ID**
- 3. National Provider ID (NPI)**
- 4. Obtain password and log-in access to SFTP site for uploading/downloading files**



# 1) Companion Guides

- Modify systems according to Companion Guides <http://hrsa.dshs.wa.gov/dshshipaa/>

## 2) PIC Crosswalk

- **ProviderOne Client IDs (not PIC ID).**
- **DSHS is providing PIC to ProviderOne Client ID crosswalk**
  - MCOs can download the crosswalk using a web applet at <https://fortress.wa.gov/dshs/npicaphrsa>
  - RSNs will get the crosswalk from the current MHD SFTP site (not the ProviderOne SFTP).
- **DSHS will email you when the crosswalk is ready.**

### 3) National Provider ID (NPI)

- **All encounter test files must use NPI**
  - This is the only way ProviderOne will identify your service providers
  - MCOs and RSNs will identify themselves to DSHS using a ProviderOne Provider ID number in the “billing or sender” identification segments
- **Taxonomy of the “pay-to-provider” will be required.**



## 4) SFTP Security

- **Using ProviderOne Secure File Transfer Protocol (SFTP) site**
  - ALL MCOs and RSNs will use the ProviderOne SFTP to submit and retrieve test files.
- **DSHS will provide each MCO and RSN**
  - SFTP website address,
  - SFTP UserID and Password
  - Organizational Submitter ID number
- **Organization must return a signed TPA in order to receive this information and before testing**

## 4) SFTP Security cont.

- ■ Once the SFTP account is established:
  - Submit your 837 encounters for format and file compliance testing to the SFTP
  - Retrieve 834 (enrollment roster) and 820 (premium payment) files from the SFTP
  - Retrieve acknowledgements, errors and reports

# Set Up ProviderOne security in addition to SFTP security

SFTP site utilized for all testing

During testing SFTP website will be used to

- Retrieve 820 and 834 transactions
- Submit 837 Encounters & receive responses

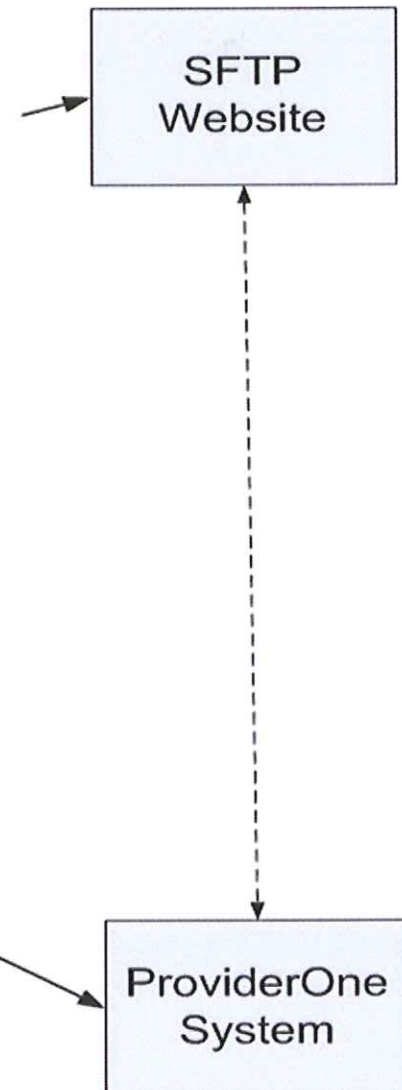
Security: SFTP passwords and UserIDs will be delivered to MCOs and RSNs



During ProviderOne training 60 days prior to implementation, MCO/RSNs will learn to

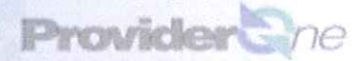
- Navigate ProviderOne
- View 834 and 820 individual transactions
- Submit FQHC/RHC rosters
- Verify Eligibility

Security: Each MCO/RSN Security Administrator logs into ProviderOne and assigns their staff appropriate security profiles





# What Comes After Testing?



- **Security Set-up** - MCO/RSN staff need security credentials (log-in and password) in order to access ProviderOne after implementation

<http://fortress.wa.gov/dshs/maa/ProviderOne/Security.htm>

## Recommended profiles

### **EXT Provider System Administrator**

(changes passwords and maintains all users for ProviderOne ID)

### **EXT Provider Managed Care Only**

(all access available to MCO and RSNs)

### **EXT Provider Eligibility Checker**

(access to verify eligibility only)

### **EXT Provider Upload and Download Files**

# What Comes After Testing?

## ■ User Training

- Participate in webinars – no travel required
- Two months before implementation
- MCO/RSN specific training will include navigation, report screens, eligibility and file upload capacities
- Eligibility verification staff can attend specific webinar trainings on this topic
- RSNs will have additional training for authorizing inpatient admissions

# Important Contacts



Topic	By Email	By Phone
Security	<a href="mailto:provideronesecurity@dshs.wa.gov">provideronesecurity@dshs.wa.gov</a>	1-800-562-3022 (option 2, then option 4, then option 1)
EDI Gateway (SFTP set-up and questions, 997 questions)	Please call for assistance	1-800-562-3022 (option 2, then option 4, option 3)
HIPAA (EDI Other) (ETRR questions)	<a href="mailto:hipaa-help@dshs.wa.gov">hipaa-help@dshs.wa.gov</a>	1-800-562-3022 (option 2, then option 4, then option 4)





# Questions?

**Visit the ProviderOne Internet**

**<http://maa.dshs.wa.gov/providerone>**